WHAT IS CLAIMED IS:

1. A method of managing invalid password attempts, said method comprising:
receiving a message from a computer system, wherein the message includes a distinguished name, the distinguished name corresponding to a failed login attempt;
calculating a total failed login attempt number corresponding to the distinguished name;
identifying a failed login attempt allowed number;
determining whether the total failed login attempt number is greater than the failed login attempt allowed number; and
revoking a password corresponding to the distinguished name based on the determination.

2. The method as described in claim 1 wherein the message is received from a plurality of servers.

3. The method as described in claim 1 further comprising:
establishing a secure connection with the computer system; and
verifying a digital certificate corresponding to the computer system, wherein the digital certificate is included in the message.

4. The method as described in claim 1 wherein the determining further comprises:
configuring parameters, wherein the parameters include a login tracking period;
storing a record in a failed login data store, the record including the distinguished name and a

timestamp corresponding to a time the message was received; and

removing one or more records from the failed login data store in response to one or more corresponding timestamps being older than the tracking period.

5. The method as described in claim 1 wherein the revoking further includes:

preparing a password revocation message, the password revocation message identifying the distinguished name; and

sending the password revocation message to one or more login servers, wherein the login servers include the computer system.

6. The method as described in claim 5 further comprising:

establishing a secure connection to each of the login servers; and

including a digital signature identifying a sending computer system in the password revocation message.

7. The method as described in claim 5 wherein the password revocation message is sent in response to determining that the password was not previously revoked; and

wherein the password revocation message is not sent in response to determining that the password was previously revoked.

8. An information handling system comprising:

one or more processors;

a memory accessible by the processors;
one or more nonvolatile storage devices accessible by the processors;
a password managing tool to process invalid password attempts, the password managing tool including:
means for receiving a message from a computer system, wherein the message includes a distinguished name, the distinguished name corresponding to a failed login attempt;
means for calculating a total failed login attempt number corresponding to the distinguished name;
means for identifying a failed login attempt allowed number;
means for determining whether the total failed login attempt number is greater than the failed login attempt allowed number; and
means for revoking a password corresponding to the distinguished name based on the determination.

9. The information handling system as described in claim 8 wherein the message is received from a plurality of servers.

10. The information handling system as described in claim 8 further comprising:
means for establishing a secure connection with the computer system; and
means for verifying a digital certificate corresponding to the computer system, wherein the digital certificate is included in the message.

11. The information handling system as described in claim 8 wherein the determining further comprises:

means for configuring parameters, wherein the parameters include a login tracking period;

means for storing a record in a failed login data store, the record including the distinguished name and a timestamp corresponding to a time the message was received; and

means for removing one or more records from the failed login data store in response to one or more corresponding timestamps being older than the tracking period.

12. The information handling system as described in claim 8 wherein the revoking further includes:

means for preparing a password revocation message, the password revocation message identifying the distinguished name; and

means for sending the password revocation message to one or more login servers, wherein the login servers include the computer system.

13. The information handling system as described in claim 12 further comprising:

means for establishing a secure connection to each of the login servers; and

means for including a digital signature identifying a sending computer system in the password revocation message.

14. A computer program product stored in a computer operable media for processing invalid password attempts, said computer program product comprising:
means for receiving a message from a computer system, wherein the message includes a distinguished name, the distinguished name corresponding to a failed login attempt;
means for calculating a total failed login attempt number corresponding to the distinguished name;
means for identifying a failed login attempt allowed number;
means for determining whether the total failed login attempt number is greater than the failed login attempt allowed number; and
means for revoking a password corresponding to the distinguished name based on the determination.

15. The computer program product as described in claim 14 wherein the message is received from a plurality of servers.

16. The computer program product as described in claim 14 further comprising:
means for establishing a secure connection with the computer system; and
means for verifying a digital certificate corresponding to the computer system, wherein the digital certificate is included in the message.

17. The computer program product as described in claim 14 wherein the determining further comprises:

means for configuring parameters, wherein the parameters include a login tracking period;
means for storing a record in a failed login data store, the record including the distinguished name and a timestamp corresponding to a time the message was received; and
means for removing one or more records from the failed login data store in response to one or more corresponding timestamps being older than the tracking period.

18. The computer program product as described in claim 14 wherein the revoking further includes:
means for preparing a password revocation message, the password revocation message identifying the distinguished name; and
means for sending the password revocation message to one or more login servers, wherein the login servers include the computer system.

19. The computer program product as described in claim 18 further comprising:
means for establishing a secure connection to each of the login servers; and
means for including a digital signature identifying a sending computer system in the password revocation message.

20. The computer program product as described in claim 18 wherein the password revocation message is sent in response to determining that the password was not previously revoked; and

wherein the password revocation message is not sent in response to determining that the password was previously revoked.